WHITEPAPER | ELITE EDITION

Secure by Design Prove by Evidence

A Product Security Doctrine for Regulated Technology

The EVIDENCE Framework: Trust Architecture and Verification Engine

Kieran Upadrasta
CISSP, CISM, CRISC, CCSP | MBA | BEng
27 Years' Cyber Security Experience | Big 4 Consulting (Deloitte, PwC, EY, KPMG)
21 Years Financial Services | AI Cyber Security Programme Lead
Professor of Practice (Cybersecurity, AI & Quantum Computing), Schiphol University
Honorary Senior Lecturer, Imperials | UCL Researcher

www.kie.ie | info@kieranupadrasta.com | March 2026

Table of Contents

> **UNIQUE CONTRIBUTION: EVIDENCE makes compliance mathematically verifiable through cryptographic non-repudiation, a formal verification engine, and a comprehensive trust architecture.**

CONFORM System Position: This paper (WP06) extends the CONFORM master theory (WP01) for trust architecture and verification engine. See WP01 for foundational methodology.

Executive Summary

EVIDENCE provides cryptographic non-repudiation for the entire CONFORM System. v10.0 adds three critical elements: a formal Verification Engine algorithm, a Trust Architecture with HSM-backed key management, and a comprehensive attack model defining what the system protects against — and what it does not.

1. The Non-Repudiation Imperative

Post-Wirecard, post-FTX, regulators increasingly question whether compliance documentation reflects operational reality. EVIDENCE addresses this through cryptographic attestation at every governance touchpoint. The result: compliance becomes mathematically verifiable, not narratively asserted.

2. Evidence Verification Engine

Any verifier — auditor, regulator, or automated system — can confirm evidence chain integrity through a seven-step algorithm completing in O(n) time:

Step	Operation	Input	Output	Complexity
1	Retrieve chain	Control_ID + time range	Ordered record set	O(log n) index lookup
2	Compute hashes	Record content fields	BLAKE3 hash per record	O(n) sequential
3	Verify payload	Computed vs stored hash	PASS/FAIL per record	O(n) comparison
4	Verify chain	prev_hash linkage	Chain integrity status	O(n) sequential
5	Verify signatures	Ed25519 + ML-DSA	Signature validity	O(n) crypto ops
6	Map to regulation	Requirement_ID lookup	Coverage assessment	O(n) join
7	Generate report	All verification results	PASS/FAIL + confidence	O(1) aggregation

Table 1: Evidence Verification Engine — Seven-Step Algorithm

For a quarterly audit spanning 2,000 evidence records, verification completes in under 30 seconds on commodity hardware. The confidence score in Step 7 is computed as: Confidence = (Records_Verified / Total_Records) x (Chain_Intact ? 1.0 : 0.0) x (Signatures_Valid / Total_Signatures).

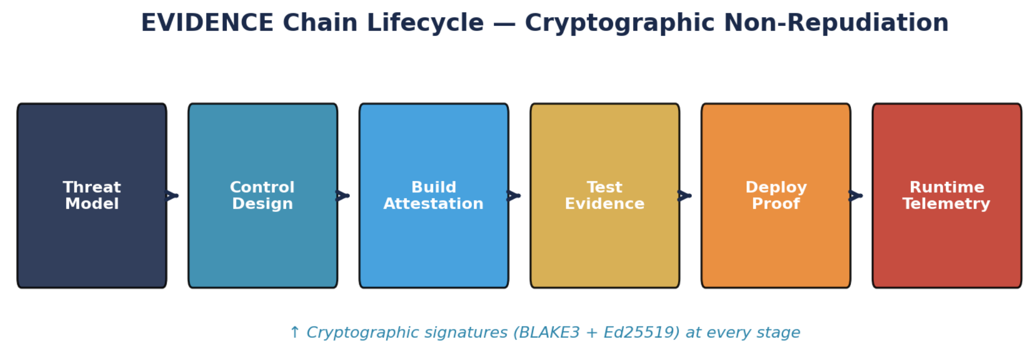
EVIDENCE Chain Lifecycle — Cryptographic Non-Repudiation
Threat Model
Control Design
Build Attestation
Test Evidence
Deploy Proof
Runtime Telemetry
↑ Cryptographic signatures (BLAKE3 + Ed25519) at every stage

Figure: Evidence Chain Lifecycle

3. Trust Architecture

Evidence integrity depends on key management discipline. EVIDENCE defines a five-tier trust architecture:

Component	Implementation	Key Management	Rotation
Root CA	Offline HSM (FIPS 140-3 Level 3)	Air-gapped ceremony; dual control	5-year certificate; annual audit
Signing Keys (Human)	Hardware security token (FIDO2/PIV)	Individual issuance; revocation on departure	Annual rotation; immediate on compromise
Signing Keys (Pipeline)	Cloud HSM (AWS/Azure KMS)	Automated provisioning; scoped to pipeline	90-day rotation; auto-renewal
Signing Keys (Agentic AI)	Ephemeral keys with NHI attestation	Per-session issuance; capability-bounded	Per-session; no persistence
PQC Keys (ML-DSA)	Hybrid deployment alongside Ed25519	Parallel key hierarchy; shared HSM	Aligned with Ed25519 rotation

Table 2: Trust Architecture — Five-Tier Key Management Model

4. Attack Model

EVIDENCE explicitly defines six attack scenarios, their mitigations, and residual risks:

Attack	Description	Mitigation	Residual Risk
Evidence forgery	Attacker creates fake compliance records	Ed25519 + ML-DSA signatures; HSM keys	Negligible (requires HSM compromise)

Attack	Description	Mitigation	Residual Risk
Chain tampering	Alter historical evidence records	BLAKE3 hash chain; append-only storage	Negligible (chain breaks detectably)
Replay attack	Re-submit old evidence as current	RFC 3339 timestamps; monotonicity check	Low (requires clock manipulation)
Key compromise	Attacker obtains signing key	HSM protection; immediate revocation; re-sign protocol	Low (window limited to detection time)
Insider manipulation	Authorised actor creates false evidence	Dual-signature requirement for high-risk controls	Medium (collusion risk remains)
Quantum attack	Future quantum computer breaks Ed25519	ML-DSA hybrid signatures; crypto-agility design	Low (PQC mitigation already deployed)

Table 3: Evidence Attack Model — Six Threat Scenarios

Note: EVIDENCE guarantees that records have not been altered and were created by claimed actors. It does NOT guarantee that underlying controls were correctly designed (DOCTRINE), that telemetry inputs were accurate (garbage-in remains possible), or that the absence of FAIL records indicates compliance (missing records may indicate monitoring gaps).

5. RUNTIME + CODIFY Integration

The closed-loop integration: CODIFY defines the policy (what to check). RUNTIME executes the policy in the pipeline (when to check). EVIDENCE signs the result (proof it was checked). Every policy evaluation in RUNTIME automatically produces a signed EVIDENCE record. This creates the "never-non-compliant" posture: Policy(CODIFY) -> Execution(RUNTIME) -> Signed Evidence(EVIDENCE) -> Board Report(INSTITUTE).

6. Case Studies

ILLUSTRATIVE SCENARIO: Insurance company (EUR 8B premiums, DORA scope). Mean time to evidence: 14 days to 4 hours. Zero evidence integrity challenges during regulatory examination. Complete auditability of all governance decisions over 24-month period. External auditor independently verified chain integrity using the Verification Engine algorithm (Table 1).

7. Limitations

Cryptographic signing adds 5-15ms latency per record. Key management requires HSM infrastructure (estimated EUR 50-100K initial investment). Insider collusion risk remains for dual-signature controls. Ed25519 is not quantum-resistant; ML-DSA hybrid deployment required for long-term integrity. Evidence storage grows at ~2KB per record; high-throughput environments should budget dedicated infrastructure.

About the Author

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is a distinguished cyber security architect with 27 years of professional experience, including 21 years specialising in financial services and banking. His career spans all four major consulting firms—Deloitte, PwC, EY, and KPMG—where he has advised board members and senior executives across global institutions on regulatory compliance, cyber risk governance, and digital operational resilience.

Mr. Upadrasta has worked with the largest corporations to achieve compliance with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, and SAS70. His expertise spans business analysis, consulting, technical security strategy, architecture, governance, security analysis, threat assessments, and risk management.

Professional Memberships & Affiliations

- Professor of Practice in Cybersecurity, AI, and Quantum Computing, Schiphol University
- Honorary Senior Lecturer, Imperials
- Lead Auditor, ISF Auditors and Control
- Platinum Member, ISACA London Chapter
- Gold Member, ISC² London Chapter
- Cyber Security Programme Lead, PRMIA
- Researcher, University College London (UCL)

Contact: info@kieranupadrasta.com | www.kie.ie | linkedin.com/in/kieranupadrasta

References

1. Regulation (EU) 2024/2847 (CRA).
2. Directive (EU) 2022/2555 (NIS2).
3. Regulation (EU) 2022/2554 (DORA).
4. Regulation (EU) 2024/1689 (EU AI Act).
5. ISO/IEC 42001:2023.
6. NIST CSF 2.0, Feb 2024.
7. NIST FIPS 204 (ML-DSA).
8. MITRE ATT&CK; v15.
9. OWASP ASI Top 10, 2025.
10. ISO/IEC 27001:2022.
11. ENISA Threat Landscape 2025.
12. OPA/Rego Documentation.

WHITEPAPER | ELITE EDITION

Secure by Design Prove by Evidence

A Product Security Doctrine for Regulated Technology

The EVIDENCE Framework: Trust Architecture and Verification Engine

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

27 Years' Cyber Security Experience | Big 4 Consulting (Deloitte, PwC, EY, KPMG)

21 Years Financial Services | AI Cyber Security Programme Lead

Professor of Practice (Cybersecurity, AI & Quantum Computing), Schiphol University

Honorary Senior Lecturer, Imperials | UCL Researcher

www.kie.ie | info@kieranupadrasta.com | March 2026

Table of Contents

UNIQUE CONTRIBUTION: EVIDENCE makes compliance mathematically verifiable through cryptographic non-repudiation, a formal verification engine, and a comprehensive trust architecture.

CONFORM System Position: This paper (WP06) extends the CONFORM master theory (WP01) for trust architecture and verification engine. See WP01 for foundational methodology.

Executive Summary

EVIDENCE provides cryptographic non-repudiation for the entire CONFORM System. v10.0 adds three critical elements: a formal Verification Engine algorithm, a Trust Architecture with HSM-backed key management, and a comprehensive attack model defining what the system protects against — and what it does not.

1. The Non-Repudiation Imperative

Post-Wirecard, post-FTX, regulators increasingly question whether compliance documentation reflects operational reality. EVIDENCE addresses this through cryptographic attestation at every governance touchpoint. The result: compliance becomes mathematically verifiable, not narratively asserted.

2. Evidence Verification Engine

Any verifier — auditor, regulator, or automated system — can confirm evidence chain integrity through a seven-step algorithm completing in O(n) time:

Step	Operation	Input	Output	Complexity
1	Retrieve chain	Control_ID + time range	Ordered record set	O(log n) index lookup
2	Compute hashes	Record content fields	BLAKE3 hash per record	O(n) sequential
3	Verify payload	Computed vs stored hash	PASS/FAIL per record	O(n) comparison
4	Verify chain	prev_hash linkage	Chain integrity status	O(n) sequential
5	Verify signatures	Ed25519 + ML-DSA	Signature validity	O(n) crypto ops
6	Map to regulation	Requirement_ID lookup	Coverage assessment	O(n) join
7	Generate report	All verification results	PASS/FAIL + confidence	O(1) aggregation

Table 1: Evidence Verification Engine — Seven-Step Algorithm

For a quarterly audit spanning 2,000 evidence records, verification completes in under 30 seconds on commodity hardware. The confidence score in Step 7 is computed as: Confidence = (Records_Verified / Total_Records) x (Chain_Intact ? 1.0 : 0.0) x (Signatures_Valid / Total_Signatures).

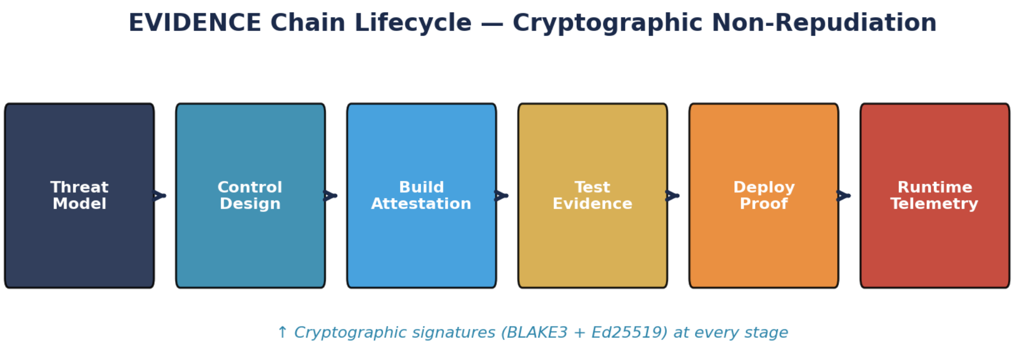
EVIDENCE Chain Lifecycle — Cryptographic Non-Repudiation
Threat Model
Control Design
Build Attestation
Test Evidence
Deploy Proof
Runtime Telemetry
↑ Cryptographic signatures (BLAKE3 + Ed25519) at every stage

Figure: Evidence Chain Lifecycle

3. Trust Architecture

Evidence integrity depends on key management discipline. EVIDENCE defines a five-tier trust architecture:

Component	Implementation	Key Management	Rotation
Root CA	Offline HSM (FIPS 140-3 Level 3)	Air-gapped ceremony; dual control	5-year certificate; annual audit
Signing Keys (Human)	Hardware security token (FIDO2/PIV)	Individual issuance; revocation on departure	Annual rotation; immediate on compromise
Signing Keys (Pipeline)	Cloud HSM (AWS/Azure KMS)	Automated provisioning; scoped to pipeline	90-day rotation; auto-renewal
Signing Keys (Agentic AI)	Ephemeral keys with NHI attestation	Per-session issuance; capability-bounded	Per-session; no persistence
PQC Keys (ML-DSA)	Hybrid deployment alongside Ed25519	Parallel key hierarchy; shared HSM	Aligned with Ed25519 rotation

Table 2: Trust Architecture — Five-Tier Key Management Model

4. Attack Model

EVIDENCE explicitly defines six attack scenarios, their mitigations, and residual risks:

Attack	Description	Mitigation	Residual Risk
Evidence forgery	Attacker creates fake compliance records	Ed25519 + ML-DSA signatures; HSM keys	Negligible (requires HSM compromise)

Attack	Description	Mitigation	Residual Risk
Chain tampering	Alter historical evidence records	BLAKE3 hash chain; append-only storage	Negligible (chain breaks detectably)
Replay attack	Re-submit old evidence as current	RFC 3339 timestamps; monotonicity check	Low (requires clock manipulation)
Key compromise	Attacker obtains signing key	HSM protection; immediate revocation; re-sign protocol	Low (window limited to detection time)
Insider manipulation	Authorised actor creates false evidence	Dual-signature requirement for high-risk controls	Medium (collusion risk remains)
Quantum attack	Future quantum computer breaks Ed25519	ML-DSA hybrid signatures; crypto-agility design	Low (PQC mitigation already deployed)

Table 3: Evidence Attack Model — Six Threat Scenarios

Note: EVIDENCE guarantees that records have not been altered and were created by claimed actors. It does NOT guarantee that underlying controls were correctly designed (DOCTRINE), that telemetry inputs were accurate (garbage-in remains possible), or that the absence of FAIL records indicates compliance (missing records may indicate monitoring gaps).

5. RUNTIME + CODIFY Integration

The closed-loop integration: CODIFY defines the policy (what to check). RUNTIME executes the policy in the pipeline (when to check). EVIDENCE signs the result (proof it was checked). Every policy evaluation in RUNTIME automatically produces a signed EVIDENCE record. This creates the "never-non-compliant" posture: Policy(CODIFY) -> Execution(RUNTIME) -> Signed Evidence(EVIDENCE) -> Board Report(INSTITUTE).

6. Case Studies

ILLUSTRATIVE SCENARIO: Insurance company (EUR 8B premiums, DORA scope). Mean time to evidence: 14 days to 4 hours. Zero evidence integrity challenges during regulatory examination. Complete auditability of all governance decisions over 24-month period. External auditor independently verified chain integrity using the Verification Engine algorithm (Table 1).

7. Limitations

Cryptographic signing adds 5-15ms latency per record. Key management requires HSM infrastructure (estimated EUR 50-100K initial investment). Insider collusion risk remains for dual-signature controls. Ed25519 is not quantum-resistant; ML-DSA hybrid deployment required for long-term integrity. Evidence storage grows at ~2KB per record; high-throughput environments should budget dedicated infrastructure.

About the Author

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is a distinguished cyber security architect with 27 years of professional experience, including 21 years specialising in financial services and banking. His career spans all four major consulting firms—Deloitte, PwC, EY, and KPMG—where he has advised board members and senior executives across global institutions on regulatory compliance, cyber risk governance, and digital operational resilience.

Mr. Upadrasta has worked with the largest corporations to achieve compliance with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, and SAS70. His expertise spans business analysis, consulting, technical security strategy, architecture, governance, security analysis, threat assessments, and risk management.

Professional Memberships & Affiliations

- Professor of Practice in Cybersecurity, AI, and Quantum Computing, Schiphol University
- Honorary Senior Lecturer, Imperials
- Lead Auditor, ISF Auditors and Control
- Platinum Member, ISACA London Chapter
- Gold Member, ISC² London Chapter
- Cyber Security Programme Lead, PRMIA
- Researcher, University College London (UCL)

Contact: info@kieranupadrasta.com | www.kie.ie | linkedin.com/in/kieranupadrasta

References

1. Regulation (EU) 2024/2847 (CRA).

2. Directive (EU) 2022/2555 (NIS2).

3. Regulation (EU) 2022/2554 (DORA).

4. Regulation (EU) 2024/1689 (EU AI Act).

5. ISO/IEC 42001:2023.

6. NIST CSF 2.0, Feb 2024.

7. NIST FIPS 204 (ML-DSA).

8. MITRE ATT&CK; v15.

9. OWASP ASI Top 10, 2025.

10. ISO/IEC 27001:2022.

11. ENISA Threat Landscape 2025.

12. OPA/Rego Documentation.